MITHRIL: Adaptable Security for Survivability in Collaborative Computing Sites

NCSA: Von Welch, Jim Basney, Himanshu Khurana
NRL CCS: Ken Hornstein
PNNL: TBD
Mithril

• Mithril is a fictional material from J.R.R. Tolkien's universe, Middle-earth. It is a precious silvery metal, **stronger** than steel but much **lighter** in weight. (from Wikipedia)

• A mithril coat of mail provides **strong** protection but is **light** and **flexible**

• Our project will develop **adaptable** site security mechanisms that **maintain usability**
Mithril

• Adaptable Security for Survivability
  – Maintain high-level of openness and usability during normal operation
  – Apply security counter-measures and adjust level of service during heavy attack

• In Collaborative Computing Sites
  – Examples: NRL Center for Computational Science (CCS), NSF centers (NCSA, SDSC, PSC, NCAR), DOE Labs (NERSC, LBNL)
Problem Statement

• Site security mechanisms cannot change quickly to respond to emerging threats
• Leads to service interruptions when serious attacks occur
• Need mechanisms for adaptable site security
Threats of Primary Concern

- Compromised accounts
  - Passwords and keys obtained from off-site compromises
  - Compromise spreads across sites
  - Large number of account compromises overwhelm manual containment practices
- Privilege escalation
- Remote exploits
Collaborative Computing Sites

- Support large, geographically distributed user communities
- Enable pooling of distributed resources
  - Single sign-on
  - Open networks
- Provide a variety of general-purpose and specialized computing services
Challenges

• Must maintain usability and openness
• Off-site users
  – Vulnerabilities outside local site control
• Research systems
  – Heterogeneity
  – Special-purpose platforms
  – Obstacles to software roll-out
Bridging the Gap
Approach

prevention → detection → response

SURVIVABILITY
Approach

Survivability Research

prevention

SURVIVABILITY
detection

response

Intrusion Detection Systems

Enterprise Security Management Systems

NCASSR Research
Existing Work

• Survivable systems research: SABER, Willow, SITAR, APOD
  – How can we bring survivability research into production?

• Enterprise Security Management Systems
  – SSH Tectia: Enterprise management of SSH services
    • Doesn’t support unique site platforms (ex. IA64 Linux)
    • Can we replicate this functionality for OpenSSH?
  – ArcSight ESM, Symantec ESM, Lightning Console, etc.
    • Are these systems applicable to our environments?

• Intrusion Detection Systems: Prelude, Snort, Tripwire, etc.
  – Mithril should integrate with these as possible
Leveraging NCASSR Y2

- Credential Management Services
- Policy and Key Management for Secure Group Communication
- SDR Policy Enforcement System
- Cluster Security (NVisionCC)
- PKI Testbed
Focus on Site Needs

- TeraGrid sites need to maintain open environment in face of targeted attacks
- NCSA is committed to an adaptable security infrastructure
- Partnership with NRL CCS
Adaptability: OTP Deployment

• One Time Password tokens are costly and inconvenient for routine use by NCSA users
• In case of sustained, large-scale attack, transition resources to high-security mode
  – Update SSH configurations to temporarily require OTP hardware token authentication
  – Distribute tokens to priority users via overnight mail
• Keep serving small number of high-priority users during intrusion response / clean-up
Project Organization

- SSH Management (Basney)
- Continuous Biometric Authentication (PNNL)
- Adaptable IDS (Welch)
- Secure Email for Incident Response (Khurana)
- Survivability Management System (Welch)
- NRL Requirements and Evaluation (Hornstein)

SURVIVABILITY

prevention -> detection

response
Managing Remote Login Services

- Remote login is arguably the most essential service provided by collaborative computing sites today
- SSH is very configurable
  - Wide variety of authentication mechanisms
  - Many options for security restrictions
- SSH can be an effective site access control point
- Plans:
  - Develop an OpenSSH management subsystem
  - Develop management system for Kerberos Telnet
SSH Key Management

- SSH public key authentication provides single sign-on
- SSH keys can be difficult to manage
  - Unencrypted or encrypted with poor passwords
  - No lifetime restrictions
  - No revocation capability
- OpenSSH credential management service
  - Delivers keys to ssh-agent, not written to disk
  - Provides revocation capabilities
Continuous Biometric Authentication

- Authenticate the user throughout their session
- Monitor mouse movement and keystroke timing
- Build on existing work at PNNL for Windows
- Apply to Unix systems

Mouse velocity distributions of different users (PNNL)
Adaptable/Reactive IDS

• Match monitoring precision with current threat level
  – Host-based IDS competes for cycles with high performance computing jobs

• Detect violations of current policy
  – Activate OTP-only policy
    -> kill non-OTP processes
Secure Email Services

- Needed for intrusion detection and coordinating intrusion response
  - Monitoring and IDS processes send alerts via email
  - Need for system administrators to communicate securely (signed, encrypted) across-site when under ongoing attack
  - Need intrusion tolerant system so attackers can’t eavesdrop

Survivability Management

• Provide a management interface to site-wide security policies
• Integrate SSH and IDS adaptation into security management console
Technology Transfer

• Design for deployment at NCSA and NRL
  – Focus on immediate needs identified by NCSA and NRL production security personnel
• Open source software distribution
• Modeling and evaluation of survivability approach for collaborative computing sites
Mithril

SURVIVABILITY

prevention

SSH key protection

detection

SSH key revocation

continuous biometric authentication

secure email

response

SSH/telnet policy changes

reactive IDS

MITHRIL: Adaptable Security for Survivability in Collaborative Computing Sites